



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/650,323	08/29/2000	Hideki Akashika	10746/20	8095

26646 7590 03/08/2004

KENYON & KENYON
ONE BROADWAY
NEW YORK, NY 10004

EXAMINER

CHEN, SHIN HON

ART UNIT PAPER NUMBER

2131

DATE MAILED: 03/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/650,323

Applicant(s)

AKASHIKA ET AL.

Examiner

Shin-Hon Chen

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 19 February 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☐ Claim(s) _____ is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-44 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 29 August 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☒ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 5.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-44 have been examined.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1, 14, 23, and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wentker et al. U.S. Pat. No. 6481632 (hereinafter Wentker) in view of Smith et al. U.S. Pat. No. 6233685 (hereinafter Smith) and further in view of Miettinen et al. U.S. Pub. 2002/0138729 (hereinafter Miettinen) and further in view of Vaeth et al. U.S. Pat. No. 6035402 (hereinafter Vaeth) and further in view of Narasimhalu et al. U.S. Pat. No. 6058383 (hereinafter Narasimhalu).

As per claim 1, 14, 23, and 36, Wentker discloses a data storing system comprising: a user apparatus which stores data (Wentker: column 1 lines 12-15: smart card); an issuing apparatus which is held by an issuer that provides the user apparatus (Wentker: column 1 lines 49-67: the issuer), a data providing apparatus which is held by a data provider that provides data (Wentker: summary: data provider provides applications). Wentker does not explicitly disclose the user apparatus comprises: registration information generation means which generates registration information on a key including a user public key or a part of a secret key, sends the

Art Unit: 2131

registration information to the issuing apparatus with user information. However, Smith discloses registration information generation means which generates registration information on a key including a user public key or a part of a secret key, sends the registration information to the issuing apparatus with user information (Smith: column 2 line 65 – column 3 line 13: the device generate public key information and send it to certification authority). It would have been obvious to one having ordinary skill in the art to combine the teachings of Smith within the system of Wentker because it allows the certificate authority to generate a certificate based on the information provided by the device to uniquely identify the device.

The combination of Wentker-Smith does not explicitly disclose an registration verification means which verifies a registration certificate, received from the issuing apparatus, which is signature information or a hash value of the issuer for the registration information and the user information, stores the registration certificate to a storage device when the registration certificate is verified. However, Miettinen discloses that limitation (Miettinen: summary: verify the certificate before storing it). It would have been obvious to one having ordinary skill in the art to combine the teachings of Wentker, Smith, and Miettinen because it prevents the system from storing unreliable or malicious certificate.

The combination of Wentker-Smith-Miettinen does not explicitly disclose an issuer registration apparatus which is held by an issuer registrar that registers and manages the issuer and the issuing apparatus comprises registration generation means which generates the registration certificate and sends the registration certificate to the user apparatus. However, Vaeth discloses that limitation (Vaeth: column 3 line 64 – column 4 line 9: registering who within an organization was authorized with signing privileges; column 6 lines 5-19: deliver the

Art Unit: 2131

certificate to the requester after the registration authority approves). It would have been obvious to one having ordinary skill in the art to combine the teachings of Wentker, Smith, Miettinen, and Vaeth because it keeps track of the people that are eligible to receive the certificate. Also, Vaeth's reference discloses "chain of trust" (Vaeth: column 41-55) which certificates are being passed down from the higher level to lower level and one with ordinary skill in the art would perceive the issuer registrar as the root certificate authority and the issuer as the second highest certificate authority and extend it individual apparatus with low level in the hierarchy.

The combination of Wentker-Smith-Miettinen-Vaeth does not explicitly disclose a data registration apparatus which is held by a data registrar that registers and manages the data provider. However, Narasimhalu discloses that limitation (Narasimhalu: column 5 lines 26-40: the information provider registers itself to the certification authority). It would have been obvious to one having ordinary skill in the art to combine the teachings of Wentker, Smith, Miettinen, Vaeth, and Narasimhalu because it helps the users to verify the certificate prior to using it.

4. Claims 2, 15, 24, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wentker in view of Miettinen and further in view of Vaeth and further in view of Narasimhalu and further in view of Lee et al. U.S. Pat. No. 6367011 (hereinafter Lee).

As per claim 2, 15, 24, and 37, Wentker discloses a data storing system comprising: a user apparatus which stores data (Wentker: column 1 lines 12-15: smart card); an issuing apparatus which is held by an issuer that provides the user apparatus (Wentker: column 1 lines 49-67: the issuer), a data providing apparatus which is held by a data provider that provides data

Art Unit: 2131

(Wentker: summary: data provider provides applications). Wentker does not explicitly disclose user apparatus comprises an registration verification means which verifies a registration certificate, received from the issuing apparatus, which is signature information or a hash value of the issuer for the registration information and the user information, stores the registration certificate to a storage device when the registration certificate is verified. However, Miettinen discloses that limitation (Miettinen: summary: verify the certificate before storing it). It would have been obvious to one having ordinary skill in the art to combine the teachings of Miettinen within the system of Wentker because it prevents the system from storing unreliable or malicious certificate.

The combination of Wentker-Miettinen does not explicitly disclose an issuer registration apparatus which is held by an issuer registrar that registers and manages the issuer and the issuing apparatus comprises registration generation means which generates the registration certificate and sends the registration certificate to the user apparatus. However, Vaeth discloses that limitation (Vaeth: column 3 line 64 – column 4 line 9: registering who within an organization was authorized with signing privileges; column 6 lines 5-19: deliver the certificate to the requester after the registration authority approves). It would have been obvious to one having ordinary skill in the art to combine the teachings of Wentker, Miettinen, and Vaeth because it keeps track of the people that are eligible to receive the certificate. Also, Vaeth's reference discloses "chain of trust" (Vaeth: column 41-55) which certificates are being passed down from the higher level to lower level and one with ordinary skill in the art would perceive the issuer registrar as the root certificate authority and the issuer as the second highest certificate authority and extend it individual apparatus with low level in the hierarchy.

Art Unit: 2131

The combination of Wentker-Miettinen-Vaeth does not explicitly disclose the issuing apparatus comprises: registration information generation means which generates registration information on a key including a user public key or a part of a secret key and generates user information; registration generation means which generates the registration certificate and sends the registration certificate to the user apparatus. However, Lee discloses that limitation (Lee: column 11 lines 11-43: generate the certificate based on card public key). It would have been obvious to one having ordinary skill in the art to combine the teachings of Wentker, Miettinen, Vaeth, and Lee because it is well known in the art to generate certificate based on public key of device or apparatus.

The combination of Wentker-Miettinen-Vaeth-Lee does not explicitly disclose a data registration apparatus which is held by a data registrar that registers and manages the data provider. However, Narasimhalu discloses that limitation (Narasimhalu: column 5 lines 26-40: the information provider registers itself to the certification authority). It would have been obvious to one having ordinary skill in the art to combine the teachings of Wentker, Miettinen, Vaeth, Narasimhalu, and Lee because it helps the users to verify the certificate prior to using it.

5. Claims 3-5, 11-13, 16, 17, 19-21, 25-27, 33-35, 38, 39, and 41-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wentker in view of Smith and further in view of Miettinen and further in view of Vaeth and further in view of Narasimhalu and further in view of Richards U.S. Pat. No. 6385723 (hereinafter Richards) and further in view of Everett et al. U.S. Pat. No. 6575372 (hereinafter Everett).

Art Unit: 2131

As per claim 3, 16, 19, 25, 38, and 41, the combination of Wentker-Smith-Miettinen-Vaeth-Narasimhalu discloses the system according to claims 1, 14, 23, and 36. Narasimhalu further discloses the user apparatus comprising: means which sends the registration certificate and storing data information to the issuing apparatus (Narasimhalu: column 5 line 60 –column 6 line 4: send the request and verification data to the CA). It would have been obvious to one having ordinary skill in the art to combine the teachings of Wentker, Smith, Miettinen, Vaeth, and Narasimhalu because it sends the it allows the certification authority to verify the requester before submitting the certificate.

Miettinen further discloses user apparatus comprises means which verifies a storing authorization when the storing authorization is received from the issuing apparatus; means which verifies that the storing data information corresponds to storing data which is acquired; and means which stores the storing data into the storage device when it is verified that the storing data information corresponds to the storing data and issuing apparatus comprises means which verifies a storing authorization which is received from the data providing apparatus (Miettinen: summary: verify the certificate before storing it). Same rationale applies here as above in rejecting claim 1. Alternatively, Richards discloses that limitation (Richards: column 10 lines 18-35 and claim 13: verify the ALC before storing it. ALC is the application load certificate which is equivalent to storing authorization). Same rationale applies here as above in combining the Miettinen reference.

The combination of Wentker-Smith-Miettinen-Vaeth-Narasimhalu does not explicitly disclose the issuing apparatus further comprising: means which verifies the registration certificate and the storing data information which are received from the user apparatus; means

Art Unit: 2131

which provides certificate information to the registration certificate and the storing data information for generating a storing authorization request when the registration certificate and the storing data information are verified; and means which sends the registration certificate, the storing data information and the storing authorization request to the data providing apparatus. However, Everett discloses that limitation (Everett: column 9 lines 6-63: the terminal first check the personalization data to make sure the card is qualified to accept the application and then the terminal and then start loading the application if verified). It would have been obvious to one having ordinary skill in the art to combine the teachings of Wentker, Smith, Miettinen, Vaeth, Narasimhalu, and Everett because it allows the system to securely check the criteria required to load applications onto the card. Everett does not explicitly disclose sending the information regarding the user apparatus to generate authorization. However, Smith discloses generating certificate based on the information provided by the user apparatus in claim 1.

Vaeth further discloses the issuing apparatus comprises and which sends the storing authorization to the user apparatus when the storing authorization is verified as disclosed in claim 1. Vaeth's reference discloses "chain of trust" (Vaeth: column 41-55) which certificates are being passed down from the higher level to lower level and one with ordinary skill in the art would perceive the data provider as the root certificate authority and the issuer as the second highest certificate authority and extend it individual apparatus with low level in the hierarchy. Therefore, the application load certificate or the storing authorization is being passed down through the hierarchy.

Vaeth further discloses the data provider comprises means which verifies the storing authorization request; means which provides certificate information to the storing authorization

Art Unit: 2131

request and the storing data information when the storing authorization request is verified for generating a storing authorization, and sends the storing authorization to the issuing apparatus (Vaeth: column 6 lines 5-19: generate certificate based on the information sent by the requester after the request has been verified). It would have been obvious to one having ordinary skill in the art to combine the teachings of Wentker, Smith, Miettinen, Vaeth, Narasimhalu, and Everett because the provider has to authenticate whether the user is eligible for receiving the data prior to transmitting it.

As per claim 4, 17, 20, 26, 39, and 42, the combination of Wentker-Smith-Miettinen-Vaeth-Narasimhalu discloses the system according to claims 1, 14, 19, 23, 36, and 41. Narasimhalu further discloses the user apparatus comprising: means which sends the registration certificate and storing data information to the issuing apparatus (Narasimhalu: column 5 line 60 – column 6 line 4: send the request and verification data to the CA). It would have been obvious to one having ordinary skill in the art to combine the teachings of Wentker, Smith, Miettinen, Vaeth, and Narasimhalu because it allows the certification authority to verify the requester before submitting the certificate.

Miettinen further discloses user apparatus comprises means which verifies a storing authorization when the storing authorization is received from the issuing apparatus; means which verifies that the storing data information corresponds to storing data which is acquired; and means which stores the storing data into the storage device when it is verified that the storing data information corresponds to the storing data and issuing apparatus comprises means which verifies a storing authorization which is received from the data providing apparatus (Miettinen: summary: verify the certificate before storing it). Same rationale applies here as above in

Art Unit: 2131

rejecting claim 1. Alternatively, Richards discloses that limitation (Richards: column 10 lines 18-35 and claim 13: verify the ALC before storing it. ALC is the application load certificate which is equivalent to storing authorization). Same rationale applies here as above in combining the Miettinen reference.

The combination of Wentker-Smith-Miettinen-Vaeth-Narasimhalu discloses the system according to claim 1. Wentker-Smith-Miettinen-Vaeth-Narasimhalu does not explicitly disclose the data providing apparatus further comprising: means which verifies the registration certificate and the storing data information which are received from the user apparatus; means which provides certificate information to the registration certificate and the storing data information for generating a storing authorization request when the registration certificate and the storing data information are verified; and means which sends the registration certificate, the storing data information and the storing authorization request to the data providing apparatus. However, Everett discloses that limitation (Everett: column 9 lines 6-63: the terminal first check the personalization data to make sure the card is qualified to accept the application and then the terminal and then start loading the application if verified). It would have been obvious to one having ordinary skill in the art to combine the teachings of Wentker, Smith, Miettinen, Vaeth, Narasimhalu, and Everett because it allows the system to securely check the criteria required to load applications onto the card. Everett does not explicitly disclose sending the information regarding the user apparatus to generate authorization. However, Smith discloses generating certificate based on the information provided by the user apparatus in claim 1.

Vaeth further discloses the data providing apparatus comprises and which sends the storing authorization to the user apparatus when the storing authorization is verified as disclosed

Art Unit: 2131

in claim 1. Vaeth's reference discloses "chain of trust" (Vaeth: column 41-55) which certificates are being passed down from the higher level to lower level and one with ordinary skill in the art would perceive the issuing apparatus as the root certificate authority and the data provider as the second highest certificate authority and extend it individual apparatus with low level in the hierarchy. Therefore, the application load certificate or the storing authorization is being passed down through the hierarchy.

Vaeth further discloses the issuing apparatus comprises means which verifies the storing authorization request; means which provides certificate information to the storing authorization request and the storing data information when the storing authorization request is verified for generating a storing authorization, and sends the storing authorization to the issuing apparatus (Vaeth: column 6 lines 5-19: generate certificate based on the information sent by the requester after the request has been verified). The functions performed by data provider and issuing apparatus can be used interchangeably because it all depends on who initiated the request to store the application to the user apparatus.

As per claim 5, 21, 27, and 43, the combination of Wentker-Smith-Miettinen-Vaeth-Narasimhalu discloses the system according to claims 1, 19, 23, and 41. Vaeth further discloses the user apparatus comprising: means which sends the registration certificate and storing data information to the data providing apparatus (Vaeth: column 6 lines 5-19). It would have been obvious to one having ordinary skill in the art to combine the teachings of Wentker, Smith, Miettinen, and Vaeth because it keeps track of the people that are eligible to receive the certificate. Also, Vaeth's reference discloses "chain of trust" (Vaeth: column 41-55) which certificates are being passed down from the higher level to lower level and one with ordinary

Art Unit: 2131

skill in the art would perceive the issuer registrar as the root certificate authority and the issuer as the second highest certificate authority and extend it individual apparatus with low level in the hierarchy.

Miettinen further discloses the user apparatus comprises means which verifies a storing authorization which is received from the data providing apparatus; means which verifies that the storing data information corresponds to storing data which is acquired; means which stores the storing data in the storage device when it: is verified that the storing data information corresponds to the storing data (Miettinen: summary: verify the certificate before storing it). It would have been obvious to one having ordinary skill in the art to combine the teachings of Wentker, Smith, Miettinen, Vaeth, and Narasimhalu because it prevents the system from storing unreliable or malicious certificate. Alternatively, Richards discloses that limitation (Richards: column 10 lines 18-35 and claim 13: verify the ALC before storing it. ALC is the application load certificate which is equivalent to storing authorization). Same rationale applies here as above in combining the Miettinen reference.

Vaeth further discloses the data providing apparatus comprises means which verifies the storing authorization request; means which generate certificate information to the storing authorization request and the storing data information when the storing authorization request is verified for generating a storing authorization, and sends the storing authorization to the user apparatus (Vaeth: column 6 lines 5-19: generate certificate based on the information sent by the requester after the request has been verified). It would have been obvious to one having ordinary skill in the art to combine the teachings of Wentker, Smith, Miettinen, Vaeth, Narasimhalu, and

Art Unit: 2131

Everett because the provider has to authenticate whether the user is eligible for receiving the data prior to transmitting it.

As per claims 11, 12, 13, 33, 34, and 35, the combination of Wentker-Smith-Miettinen-Vaeth-Narasimhalu-Everett discloses the system according to claims 3-5 and 25-27. Wentker further discloses the user apparatus further comprising means which deletes the storing data which is in the storage device (Wentker: column 2 lines 33-52).

6. Claims 6, 18, 28, and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wentker in view of Smith and further in view of Miettinen and further in view of Vaeth and further in view of Narasimhalu and further in view of Lee and further in view of Takahashi et al. U.S. Pat. No. 6377692 (hereinafter Takahashi).

As per claim 6, 18, 28, and 40, the combination of Wentker-Smith-Miettinen-Vaeth-Narasimhalu discloses the system according to claims 1, 14, 23, and 36. Vaeth further discloses the issuing apparatus comprises means which sends information used for providing certificate information to the issuer registration apparatus (Vaeth: column 3 line 64 – column 4 line 9: registering who within an organization was authorized with signing privileges; column 6 lines 5-19: deliver the certificate to the requester after the registration authority approves). It would have been obvious to one having ordinary skill in the art to combine the teachings of Wentker, Smith, Miettinen, Vaeth, and Narasimhalu because it keeps track of the people that are eligible to receive the certificate. Also, Vaeth's reference discloses "chain of trust" (Vaeth: column 41-55) which certificates are being passed down from the higher level to lower level and one with ordinary skill in the art would perceive the issuer registrar as the root certificate authority and the

Art Unit: 2131

issuer as the second highest certificate authority and extend it individual apparatus with low level in the hierarchy.

Miettinen further discloses issuing apparatus comprises means which verifies an issuer registration certificate which is received from the issuer registration apparatus; means which stores the issuer registration certificate when the issuer registration certificate is verified and the user apparatus further comprising: means which verifies the registration certificate and the issuer registration certificate which are received from the issuing apparatus; and means which stores the registration certificate and the issuer registration certificate into the storage device when the registration certificate and the issuer registration certificate are verified. (Miettinen: summary: verify the certificate before storing it). Same rationale applies here as above in rejecting claim 1.

The combination of Wentker-Smith-Miettinen-Vaeth-Narasimhalu does not explicitly disclose the issuing apparatus comprises means which stores the issuer registration certificate when the issuer registration certificate is verified; means which generates the registration certificate to the user apparatus, and sends the registration certificate to the user apparatus with the issuer registration certificate. However, Lee discloses that limitation (Lee: column 11 lines 11-43: generate the certificate based on card public key... card certificate and issuer certificate and secret key are placed into the card record). It would have been obvious to one having ordinary skill in the art to combine the teachings of Wentker, Smith, Miettinen, Vaeth, Narasimhalu, and Lee because it is well known in the art to generate certificate based on public key of device or apparatus.

The combination of Wentker-Smith-Miettinen-Vaeth-Narasimhalu-Lee does not explicitly disclose the issuer registration apparatus further comprising: means which provides

Art Unit: 2131

certificate information to the information used for providing the certificate information for generating the issuer registration certificate, and sends the issuer registration certificate to the issuing apparatus. However, Takahashi discloses that limitation (Takahashi: background art and column 5 line 35 – column 6 line 12: send the member register certificate to the members). It would have been obvious to one having ordinary skill in the art to combine the teachings of Wentker, Smith, Miettinen, Vaeth, Narasimhalu, Lee, and Takahashi because provide unique certificate to each member so that they can carry out the transactions in a secure manner.

7. Claims 7-10, 22, 29-32, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wentker in view of Smith and further in view of Miettinen and further in view of Vaeth and further in view of Narasimhalu and further in view of Everett and further in view of Takahashi.

As per claim 7, 8, 9, 22, 29-31, and 44, the combination of Wentker-Smith-Miettinen-Vaeth-Narasimhalu-Everett discloses the system according to claims 3-5, 19, 25-27, and 41. Narasimhalu further discloses the data providing apparatus comprises means which sends information used for providing certificate information to the data registration apparatus (Narasimhalu: column 5 lines 16-40: provider register to the certification authority). Same rationale applies here as above in rejecting claim 1. Narasimhalu also discloses the data providing apparatus comprises means which generates storing data with certificate information wherein the certificate information is provided to the storing data, and adds the data provider registration certificate to the storing data with certificate information (Narasimhalu: column 6 lines 23-31: verify the received data using the certificate received from the provider; it implies that the provider sends the certificate information along with the data to the user). It would have

Art Unit: 2131

been obvious to one having ordinary skill in the art to combine the teachings of Wentker, Smith, Miettinen, Vaeth, Narasimhalu, and Everett because it allows the user to verify the integrity of the data.

Miettinen further discloses data providing apparatus comprises means which verifies data provider registration certificate received from the data registration apparatus, and stores the data provider registration certificate when the data provider registration certificate is verified and the user apparatus further comprising means which verifies the storing data with certificate information which is received from the data providing apparatus by using the data provider registration certificate, and stores the storing data into the storage device when the storing data with certificate information is verified (Miettinen: summary: verify the certificate before storing it). Same rationale applies here as above in rejecting claim 3.

The combination of Wentker-Smith-Miettinen-Vaeth-Narasimhalu-Everett does not explicitly disclose the data registration apparatus comprises means which generates the data provider registration certificate wherein certificate information is added to the information which is received from the data providing apparatus, and sends the data provider registration certificate to the data providing apparatus. However, Takahashi discloses that limitation (Takahashi: background art and column 5 line 35 – column 6 line 12: send the member register certificate to the members). It would have been obvious to one having ordinary skill in the art to combine the teachings of Wentker, Smith, Miettinen, Vaeth, Narasimhalu, Everett, and Takahashi because provide unique certificate to each member so that they can carry out the transactions in a secure manner.

Art Unit: 2131

As per claim 10 and 32, the combination of Wentker-Smith-Miettinen-Vaeth-Narasimhalu-Everett discloses the system according to claims 3 and 25. Narasimhalu further discloses the data providing apparatus comprises means which sends information used for providing certificate information to the data registration apparatus (Narasimhalu: column 5 lines 16-40: provider register to the certification authority). Same rationale applies here as above in rejecting claim 3. Narasimhalu also discloses the data providing apparatus comprises means which generates storing data with certificate information wherein the certificate information is provided to the storing data, and adds the data provider registration certificate to the storing data with certificate information (Narasimhalu: column 6 lines 23-31: verify the received data using the certificate received from the provider; it implies that the provider sends the certificate information along with the data to the user). It would have been obvious to one having ordinary skill in the art to combine the teachings of Wentker, Smith, Miettinen, Vaeth, Everett and Narasimhalu because it allows the user to verify the integrity of the data.

Miettinen further discloses data providing apparatus comprises means which verifies data provider registration certificate received from the data registration apparatus, and stores the data provider registration certificate when the data provider registration certificate is verified and the user apparatus further comprising means which verifies the storing data with certificate information which is received from the data providing apparatus by using the data provider registration certificate, and stores the storing data into the storage device when the storing data with certificate information is verified (Miettinen: summary: verify the certificate before storing it). Same rationale applies here as above in rejecting claim 3.

Art Unit: 2131

The combination of Wentker-Smith-Miettinen-Vaeth-Narasimhalu-Everett does not explicitly disclose the data registration apparatus comprises means which generates the data provider registration certificate wherein certificate information is added to the information which is received from the data providing apparatus, and sends the data provider registration certificate to the data providing apparatus. However, Takahashi discloses that limitation (Takahashi: background art and column 5 line 35 – column 6 line 12: send the member register certificate to the members). It would have been obvious to one having ordinary skill in the art to combine the teachings of Wentker, Smith, Miettinen, Vaeth, Narasimhalu, and Takahashi because provide unique certificate to each member so that they can carry out the transactions in a secure manner. Claim 10 discloses the data registration apparatus generates data certificate instead of data provider registration certificate as claimed in claims 7-9. Everett further discloses that limitation (Everett: column 13 line 66 – column 14 line 15: issuing application certificate). It would have been obvious to one having ordinary skill in the art to combine the teachings of Wentker, Smith, Miettinen, Narasimhalu, Vaeth, Everett, and Takahashi because it allows the system to specifically load a unique application identified by unique application load certificate.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

* The prior art by Wentker achieves the goal the applicant wishes to achieve through different method.

Art Unit: 2131

Everett et al. U.S. Pat. No. 6488211 discloses system and method for flexibly loading in IC card.

Sehr U.S. Pat. No. 6325292 discloses card system and methods utilizing collector cards.

Taylor U.S. Pat. No. 5530232 discloses multi-application data card.

Tamada et al. U.S. Pat. No. 5729717 discloses IC card and issuing apparatus allowing multiple applications.

Susaki et al. U.S. Pat. No. 6253322 discloses electronic certification authentication method and system.

Deindl et al. U.S. Pat. No. 6173401 discloses importing information onto a chip card.

Asay et al. U.S. Pub. No. US2001/0011255 discloses reliance management for electronic transaction system.

Patel et al. U.S. Pat. No. 6438690 discloses vault controller based registration application serving web based registration authorities and end users for conducting electronic commerce in secure end-to-end distributed information system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (703) 305-8654. The examiner can normally be reached on Monday through Friday 8:00am to 4:30pm.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shin-Hon Chen
Examiner
Art Unit 2131

SC


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100